SECURITY INTEGRATED CIRCUIT

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to an integrated circuit for processing received transmitted signals, in particular broadcast signals such as television.

Description of the Related Art

A wide variety of techniques for broadcast transmission are known in which the broadcast signal is encoded, scrambled or encrypted in some way to allow only authorized recipients to retrieve the original signal. One particular field in which this area has been researched is broadcast television.

The broadcast of television signals in which only permitted or authorized recipients can produce the clear television picture from those signals is known as Conditional Access Television or Pay-TV. In this context, broadcast can include over-air, via satellite, by cable or indeed any appropriate distribution medium in which the same signal content is sent to many recipients. Television signals may be analogue signals or digital signals. The term "scrambling" is often used for the process of rendering analogue signals unusable until "descrambled", whereas the terms "encryption" and "decryption" are more often used for digital signals. In either case, the aim is to only allow users that have paid a subscription to descramble/decrypt the signals.

A known system and receiver for processing received signals is described in EP 0,428,252 which is illustrated in Figure 1. The concept in this system is to broadcast signals in the air (by satellite) that can be received by anyone, but only rendered usable by recipients having a "set top box" decoder 2 and an associated smart card 22. The decoders 2 of all recipients are identical, but the smart cards 22 contain unique secrets, including entitlements, which

specify which channels within the broadcast signals the user is permitted to watch. The system operates broadly as follows:

A television signal is broadcast over air in a scrambled form and includes a stream of control data describing how the television signal is to be descrambled. The television signals and control data are necessarily the same signal sent to all users. It is not feasible to send the signals uniquely scrambled/encrypted to each recipient as there may be tens of millions of users and this would require tens of millions of times the bandwidth. Accordingly, all recipients must be able to operate the same descrambling/decryption process. This is implemented in the decoder 2, which receives the broadcast signals from a receiver 12. A data demodulator 14 extracts the portion of the signal for picture and/or sound and provides this to a descrambler 16 for descrambling. The control data portion is extracted and provided to a verifier 20 over line 15. The control data comprises encrypted control words that are needed to instruct the descrambler how to descramble the picture/sound signal. The control words must therefore be decrypted, and it is for this purpose that the smart card 22 is provided.

The verifier 20 provides encrypted control words across an interface along line 21 to the smart card 22. The smart card 22 contains an algorithm that, if the user is entitled to watch the chosen channel, decrypts the control words and provides them to the verifier 20 via line 23. The verifier passes the decrypted control words to a PRBS 18, which in turn provides a descrambling code to the descrambler. It should be noted that the control words and hence the descrambling code change frequently (every few seconds). The security in this arrangement makes it infeasible to try and decrypt the control words in real time without the smart card algorithm. Also, in the event the smart card algorithm is compromised, then the smart cards themselves can be re-issued to all subscribers. Lastly, to view any channels, a user must pay for "entitlements" that are broadcast over air and addressed uniquely to each user and stored in the smart card 22.

A second published system is disclosed in a paper "Security and Addressability for Pay-TV" given at The Video Revolution Conference July 1982, University of Reading. In this system, it is proposed that a monthly key is broadcast to each subscriber using each subscriber's unique unit key stored in a decoder. In turn the monthly key, which is common to all users of the system, is used to decrypt a program key for decrypting a given television program.

BRIEF SUMMARY OF THE INVENTION

We have appreciated security problems with known conditional access broadcast techniques. In the smart card approach, the decrypted control words are available across an open interface between the smart card and decoder. These can be recorded and provided to other users by another communication channel (such as the Internet) and any recipient is thereby enabled to descramble the broadcast signal.

In accordance with one embodiment of the invention, a semiconductor integrated circuit for decryption of broadcast signals is provided that includes an input interface for receipt of received encrypted broadcast signals and control data and an output interface for output of decrypted broadcast signals; an input interface for receipt of received encrypted broadcast signals and control data, and an output interface for output of decrypted broadcast signals; a processing unit arranged to receive encrypted broadcast signals via the input interface, to decrypt the encrypted broadcast signals in accordance with control signals, and to provide decrypted broadcast signals to the output interface; a first decryption circuit arranged to receive encrypted control signals from the input interface and to decrypt the control signals in accordance with a common key from a common key store; a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store; whereby the circuit is arranged such that the only route to placing a common key in the common key

store is to input the common key in encrypted form for decryption in accordance with the secret key, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

In accordance with another embodiment of the invention, a decryption device is provided that includes a common key store configured to receive a common key in encrypted form; a secret key store configured to store a secret key; a decryption unit comprising a first decryption circuit configured to receive encrypted control signals and to decrypt the control signals in accordance with a common key from the common key store, and a second decryption circuit configured to receive the common key in encrypted form and to decrypt the common key in accordance with a secret key from the secret key store and to store the common key in the common key store; and a processing unit configured to receive encrypted broadcast signals and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit and to provide decrypted broadcast signals to an output interface.

A method for decryption of broadcast signals is provided, the method includes the steps of receiving encrypted broadcast signals, encrypted control signals, and encrypted common key signals at an input interface of a decryption unit formed on a semiconductor integrated circuit; decrypting the encrypted common key utilizing a stored secret key to generate a common key; decrypting the encrypted control signals with the common key to generate decrypted control signals; and decrypting the encrypted broadcast signals in accordance with the control signals and providing decrypted broadcast signals to an output interface of the decryption device.

In accordance with another embodiment of the invention, a method for broadcasting signals is provided. The method includes encrypting control words and transmitting the encrypted control words; encrypting a common key and transmitting the encrypted common key; encrypting broadcast signals and

transmitting the encrypted broadcast signals to the plurality of subscribers; providing a secret key to the authorized recipients that is stored in a decryption unit; receiving encrypted broadcast signals, encrypted control signals, and encrypted common key signals at an input interface of a decryption unit formed on a semiconductor integrated circuit; decrypting the encrypted common key utilizing a stored secret key to generate a common key; decrypting the encrypted control signals with the common key to generate decrypted control signals; and decrypting the encrypted broadcast signals in accordance with the control signals and providing decrypted broadcast signals to an output interface of the decryption device.

In accordance with yet another embodiment of the invention, a system for broadcasting signals to a plurality of subscribers is provided. The system includes a transmitter configured to broadcast signals encrypted according to control words, control words encrypted according to a common key that is common to all authorized recipients, and a common key encrypted according to a secret key that is unique to each authorized recipient; and a plurality of receivers to receive the broadcast signals, each receiver comprising a decryption unit having a secret key unique to the decryption unit stored therein, and each decryption unit further comprising: a common key store configured to receive a common key in encrypted form; a secret key store configured to store a secret key; a decryption unit comprising a first decryption circuit configured to receive encrypted control signals and to decrypt the control signals in accordance with a common key from the common key store, and a second decryption circuit configured to receive the common key in encrypted form and to decrypt the common key in accordance with a secret key from the secret key store and to store the common key in the common key store; and a processing unit configured to receive encrypted broadcast signals and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit and to provide decrypted broadcast signals to an output interface.

The preferred embodiment of the invention has the advantage that no data is exposed, which could allow the security to be compromised.

BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention will now be described by way of example only with reference to the figures, in which:

Figure 1 shows a known receiver and decoder arrangement; and

Figure 2 shows the main functional components of a circuit embodying the invention.

DETAILED DESCRIPTION OF THE INVENTION

A semiconductor integrated circuit 30 embodying the invention is shown in Figure 2. In the illustrated embodiment, of importance is that the circuit 30 is a monolithic device in the sense that it is implemented as a single chip with the result that the internal bus connections shown are not available to exterior devices. It is not possible, therefore, for a hacker to compromise the security of the arrangement by simply reading the signals on any of the internal buses. The only external connections are at input interface 43, which receives the broadcast signal and output interface 45 which provides the descrambled/decrypted output signal. The embodiment is primarily applicable to digital broadcast television signals (broadcast by any medium), but is equally applicable to any other digital broadcast signal where security is required.

A digital television signal is received by a receiver, processed according to how the signal was received (*e.g.,* satellite, terrestrial, cable) and is demultiplexed from data signals including a control channel. The resultant digital TV signal remains in encrypted form, and is provided to the circuit 30 at interface 43. The TV signal is necessarily encrypted according to an encryption/decryption scheme common to all authorized recipients. This is because there are likely to be millions of recipients, and to broadcast the TV signal using individual encryption

schemes would require broadcasting the signal in millions of different encrypted forms simultaneously, and this is simply not feasible. The encrypted TV signal is provided to a DVB unit 38 on an internal bus line 45, where it is decrypted in accordance with control data to produce a clear TV signal at an output line 41 to output interface 45. The clear TV signal is a digital data stream that can be converted to picture and sound without further secret cryptographic techniques.

A fixed decryption scheme could be used having a key common to all users; however, this would be insecure because once deciphered, the decryption would then be available to all. Accordingly, a changing encryption scheme is used in which an encrypted flow of control words (CW) are broadcast in the control data, which requires decryption to be provided to the DVB Unit 38. The control words are also encrypted in a manner common to all authorized recipients, otherwise a unique flow of control words would need to be individually provided to each of the millions of recipients, which would again be infeasible because of bandwidth. The control words are provided in encrypted form via an input interface 43 and internal bus 47 to a decryption circuit 32, preferably an AES circuit. The AES circuit 32 decrypts the encrypted control words and provides it to the DVB unit 38 via the internal bus 31.

The encryption scheme of the control word data flow is the same for all recipients (otherwise the control word data flow itself would differ for each recipient with the bandwidth problem noted above). A Common Key (CK) for the AES circuit 32 is therefore required. The common key (CK), we have appreciated, could present a weakness in the security of the whole system. If the common key could be found and provided to the circuit 30 then, once deciphered, any user could simply provide the common key to their set top box (in which the circuit 30 is located) and would then have free access.

The circuit 30 is therefore arranged to avoid this weakness. The common key (CK) is broadcast as part of the control data in encrypted form. Now, the common key could be used with a given program, with different common keys

associated with different programs. Thus, new common keys need to be broadcast at the rate of a few per hour. In preference, though, the key is used for a limited time period (*e.g.*, weeks, months). The common keys are broadcast encrypted using secret keys unique to each circuit, and so are broadcast in millions of different encrypted forms (one form to each recipient). As each key is a 128 bit string, and only a few are required per month (say 10), then for 10 million subscribers, the data rate required is of the order kilobits per second. The encrypted common keys (CK) are received and provided to the input interface 43 and then to the AES decryption circuit 32 on line 49. A secret key in the secret key store 34 is retrieved and also provided to the AES decryption circuit 32 on an internal bus 35. The decryption circuit 32 then decrypts the appropriate encrypted common keys and provides these on the internal bus 33 to a common key store 36. The common key store is formed as a table with a program ID (PID) and associated common key (CK) stored associated with one another. The appropriate CK can then be selected for a related received program identified by its PID. Preferably, multiple PIDs will be associated with each CK. The use of multiple common keys in this way allows different levels of service to be provided depending on the service paid for and hence the keys provided.

It is to be noted that the only way of providing control words to the DVB unit 38 is through the decryption circuit 32, and so even if the control words were known for a given program, the circuit could not be used without knowing the common key. In any event, the control words are not exposed at any outside interface, and so it is very unlikely that they could become known. It is further noted that the only way of providing the common key to the decryption circuit 32 is to pass the encrypted common key through the decryption circuit 32 itself under control of the secret key. Thus, if the common key for a particular program became known, the circuit 30 could still not be used to decrypt the program without knowing the secret key. Even if the secret key of a given circuit were known, this would only allow that circuit to be used, but no other. The circuit is therefore very

secure to hacking. The secret keys are chosen to be unique to each circuit having no discernible relationship to an address of the circuit.

Although shown as a single decryption circuit 32, two such circuits could be provided, one for CW decryption, and the other for CK decryption. Of course, more than one secret key could also be used in each circuit and such modifications are within the scope of the invention.

All of the above U.S. patents, U.S. patent application publications, U.S. patent applications, foreign patents, foreign patent applications and non-patent publications referred to in this specification and/or listed in the Application Data Sheet, are incorporated herein by reference, in their entirety.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims and the equivalents thereof.